Substance of Interview

Applicants' would firstly like to thank examiner Abdulhakim Nobahar and his supervisor Gilberto Barron for granting a personal interview on August 29, 2005. As a result of the interview, it was agreed that claim 5 defines over the prior art of Harif. It was also agreed that the Applicants' would propose to amend claim 1 to more clearly set forth the relationship between the External and Central entities with respect to authentication of the User. In response, Applicants' have amended claim 1 to include similar language as claim 5 to clarify this relationship and submit that no new matter has been added. In addition, Applicants' have amended claims 2 and 3 for formality reasons. Also during the interview, the Applicants' emphasized that "digital identity" as set forth in the claims and described in the specification is operationally different and distinct from prior art authentication techniques. Further elaboration on such differences follows.

Remarks

Claims 1-5 are pending in this application. Claims 1-5 stand rejected by Harif (U.S. Patent Publication No. 2002/0087881; hereafter "Harif"). Claims 1-3 are amended herewith. The prior art rejections are addressed below.

Rejections under 35 U.S.C. 102

Claims 1-5 were rejected under 35 USC 102(e) as being anticipated by Harif (2002/0087881). These rejections are respectfully traversed.

To anticipate a claim, the reference must teach every element of the claim: "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See MPEP 2131. This standard has not been met in the present case for the following reasons.

Specific differences between the claims and the cited prior art are discussed below:

With respect to claim 1, Harif does not identify or authenticate Users or individuals in e-commerce using digital identity.

In Harif, task identities are assigned to tasks, and digital signatures provided to computational devices – not to Users: Harif identifies a plurality of tasks requested by a network client with a unique identifier, or task ID: "[f]or privacy purposes, each task receives a unique identifier to be used until the task completes processing." See [0052]. In paragraphs [0029] and [0030], Harif discloses that the network client 12 as shown in figure 1 corresponds to a computational device which may be, for example, a personal computer. According to Harif, upon

initially joining the heterogenous network, each such computational device is certified by the FRC with a digital signature [0050]. In paragraph [0053], Harif again states that the digital signature (which may include a digital certificate) authenticates computational devices.

Even if the network client of Harif corresponded to a User, the "external-entity" would be incapable of positively identifying such User. Harif repeatedly teaches that the identities of the network client, network server and network host all remain anonymous, or unknown, to one another [0042], [0047], [0050]. Thus, Harif does not positively identify a User or individual as claimed.

The task ID and digital signature of Harif are different from digital identity. The digital identity of the current invention presents a unique identification and authentication mechanism as set forth for example on page 5 lines 15-18 of the specification (and consistent with Applicants' remarks filed 04/27/2005) that is different from prior art techniques. In addition, the specification makes it clear that (as opposed to e.g., digital certificates and task IDs which involve installing or downloading software/program instructions on a computer) all that is required for positive identification or authentication are the three disclosed "entities" in communication with one another and digital identity. Thus, the present invention actually provides a highly simplified and cost-effective mechanism for implementing User identification and authentication into the marketplace. Even more, unlike the task identifier of Harif, the digital identity does not require an existing relationship between the User and External-Entity and thereby expands the scope of businesses that are able to authenticate the User beyond those that are "certified members" of a heterogenous network (cf. Harif [0050]).

Thus, because the system Harif does not positively identify Users and the task identity and digital signature of Harif do not correspond to, and are inconsistent with digital identity, Applicants' submit that claim 1 is allowable over the prior art.

Regarding claim 2, Harif does not disclose providing the User with a digital identity that includes SecureCode and other information such as UserName.

The SecureCode of the present invention is described for example on page 5 lines 15-18 and page 13 line 24 – page 15 line 4 of the specification. The SecureCode is a component of the digital identity which either on its own, or combined with other information such as UserName, allows a User to be positively identified or authenticated in e-commerce. Harif does not disclose such a digital identity, SecureCode or UserName that positively identifies a User in e-commerce, but rather uses a digital signature or task ID to identify either a computational device or task. See [0050] and [0052]. Accordingly, Applicant's submit that claim 2 is allowable either on its own and/or because it depends from claim 1.

With respect to claim 3, Harif does not disclose providing a User with a SecureCode that is dynamic, non-predictable and time dependent.

PAGE 6/10 * RCVD AT 8/30/2005 3:17:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/35 * DNIS:2738300 * CSID:703 968 8877 * DURATION (mm-ss):03-08

On page 4 of the office action mailed 07/15/2005 it was asserted that the one-time password of Harif corresponds to the recited time dependent alphanumeric code [0036], and the unique identifier corresponds to the recited dynamic, non-predictable SecureCode [0052]. Applicants' respectfully disagree.

Firstly, the one-time password and unique identifier of Harif do not identify a User as does the claimed invention. Secondly, the one time password and unique identifier are not even used together and therefore cannot be combined to meet the dynamic, non-predictable and time dependent requirements of the SecureCode. For example, the one-time passwords addressed in paragraph [0036] are not provided to the network client, but to outside processors in order to access the network client's resources. On the other hand, the unique identifier associated with the taskID is provided to the network client to identify an individual task (wherein single-use authentication associated therewith is assigned "directly to the resource request associated with the task" – not to a user). See [0052].

In contrast, the SecureCode of the present invention is novel in that it is formulated (e.g., using a proprietary algorithm) such that it is computationally infeasible to detect any pattern or User information - rendering it entirely non-guessable and non-predictable. Moreover, unlike passwords, it is impossible for any two or more people to have the same SecureCode. In this way, the SecureCode is capable of being used alone for authentication or is able to be uniquely combined with other User information as a second factor.

Thus, Harif does not disclose providing a SecureCode to a User and that is further dynamic, non-predictable and time dependent as claimed. Accordingly, Applicants' submit that claim 3 is allowable over the prior art on its own and/or because it ultimately depends from claim 1.

Regarding claim 4, Applicant's submit that because claim 1 is allowable over the prior art, claim 4 is also allowable because it depends from claim 1.

With respect to claim 5, Harif does not identify or authenticate Users or individuals in e-commerce using digital identity.

<u>In Harif, task identities are assigned to tasks, and digital signatures provided to computational devices – not Users:</u> Harif identifies a plurality of tasks requested by a network client with a unique identifier, or task ID: "[f]or privacy purposes, each task receives a unique identifier to be used until the task completes processing." See [0052]. In paragraphs [0029] and [0030], Harif discloses that the network client 12 as shown in figure 1 corresponds to a computational device which may be, for example, a personal computer. According to Harif, upon initially joining the heterogenous network, each such computational device is certified by the FRC

with a digital signature [0050]. In paragraph [0053], Harif again states that the digital signature (which may include a digital certificate) authenticates computational devices.

Even if the network client of Harif corresponded to a User, the "external-entity" would be incapable of positively identifying such User. Harif repeatedly teaches that the identities of the network client, network server and network host all remain anonymous, or unknown, to one another [0042], [0047], [0050]. Thus, Harif does not positively identify a User or individual as claimed.

The task ID and digital signature of Harif are different from digital identity. The digital identity of the current invention presents a unique identification and authentication mechanism as set forth for example on page 5 lines 15-18 of the specification (and consistent with Applicants' remarks filed 04/27/2005) that is different from prior art techniques. In addition, the specification makes it clear that (as opposed to e.g., digital certificates or task IDs which require the user to install software or program instructions on their computer) all that is required for positive identification or authentication are the three disclosed "entities" in communication with one another and the digital identity. Thus, the present invention actually provides a highly simplified and cost-effective mechanism for implementing User identification and authentication into the marketplace. Even more, unlike the task identifier of Harif, the digital identity does not require an existing relationship between the User and External-Entity and thereby expands the scope of businesses that are able to authenticate the User beyond those that are members of a heterogenous network (cf. Harif [0050]).

Further regarding claim 5, Harif does not disclose an External-Entity requesting a User to authenticate himself using SecureCode or digital identity.

Nowhere does Harif disclose a User submitting SecureCode or digital identity to the External-Entity. As set forth for example on page 5 lines 15-18 and page 13 line 24 – page 15 line 4 of the specification, the SecureCode of the present invention is a component of the digital identity which either on its own, or combined with other information such as UserName, allows a User to be positively identified or authenticated in e-commerce. Harif does not disclose a digital identity, SecureCode or UserName that positively identifies a User in e-commerce, but rather uses a digital signature or task ID to identify either a computational device or task. See [0050] and [0052].

Further regarding claim 5, Harif does not disclose a SecureCode that is dynamic, non-predictable and time dependent.

On page 5 of the office action mailed 07/15/2005 it was asserted that the one-time password of Harif corresponds to the recited time dependent alphanumeric code [0036], and the unique identifier corresponds to the recited dynamic, non-predictable SecureCode [0052]. Applicants' respectfully disagree.

Firstly, the one-time password and unique identifier of Hanif do not identify a User as does the present invention as claimed. Secondly, the one time password and unique identifier are not even used together and therefore cannot be combined to meet the dynamic, non-predictable and time dependent requirements of the SecureCode. For example, the one-time passwords addressed in paragraph [0036] are not provided to the network client, but to outside processors in order to access the network client's resources. On the other hand, the unique identifier associated with the taskID is provided to the network client to identify an individual task (wherein single-use authentication is assigned "directly to the resource request associated with the task" – not to a user). See [0052].

In contrast, the SecureCode of the present invention is novel in that it is formulated (e.g., using a proprietary algorithm) such that it is computationally infeasible to detect any pattern or User information therein - rendering it entirely non-guessable and non-predictable. Moreover, unlike passwords, it is impossible for any two or more people to have the same SecureCode. In this way, the SecureCode is capable of being used alone for authentication or is able to be uniquely combined with other User information as a second factor.

Thus, Hanif does not disclose providing a SecureCode to a User that is dynamic, non-predictable and time dependent as claimed.

For the above described reasons, Applicants' respectfully submit that claim 5 is allowable over the prior art.

Conclusion

Accordingly, Applicants' respectfully request reconsideration of the claim rejections based on the above amendments and remarks. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. If the examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (571) 228-2938.

Respectfully submitted,

Dated: 08/30/2005

By: _____

Shawna J. Shaw
Agent for Applicants
Registration No. 57,091